THE JACOBS REPORT

GILDA Z. JACOBS
MICHIGAN SENATE
Assistant Democratic Floor Leader
FOURTEENTH DISTRICT

For Immediate Release
September 29, 2006

Contact: Matt Levin
(517) 373-7888

SCHOOL DISTRICTS SUE STATE

Claim Fingerprinting Is Unfunded Mandate

A coalition of 463 school districts is suing the state, claiming that the Student Safety Act violates the Headlee Amendment by requiring employee fingerprinting without providing funding to do so.

The Student Safety Act, a package of 18 bills, was passed by the Legislature last year. The legislation, which was signed into law by the governor, was designed to keep sex offenders away from schools. Part of the package mandated that school districts fingerprint and do background checks on employees to safeguard against employment of convicted sex offenders.

Problems arose immediately after the bills became law. Employees with old underage drinking tickets from high school were getting added to the list of offenders. Names were confused. Innocent people found their names listed for no apparent reason. The education community banded together, urging the Legislature to design greater list filters, which it did.

In May, whispers of a Headlee violation began circulating. The Headlee Amendment specifically prohibits state government from imposing unfunded mandates on schools.

The schools argue that the new law forces them to pay a minimum $65 per employee for fingerprints and background checks.

The House did set aside $3.7 million in the Fiscal Year (FY) 2007 budget reimbursements, but the schools point out that the money only covered the costs of the fingerprint checks after the state botched the first round earlier this year.

“No one is arguing the validity or merit of this law,” said Dennis Pollard, attorney for the group suing the state, Keep the Promise to Michigan’s Children. “Legislation that looks to protect our children, teachers and staff is something we can all agree is needed. But each new mandate handed down to school districts without the necessary funding costs our schools and eventually will cost our students. Well-intentioned mandates come at a million-dollar price.”

For example, the new mandate will cost the Saginaw School District more than $136,000 in the next two years to fingerprint about 1,800 employees and 3,000 volunteers. The district faced a $7 million deficit this summer.

The Michigan Department of Education is currently reviewing the new lawsuit.

DOCTORS ENDORSE GOVERNOR'S HEALTH PLAN

MSMS: Coverage Fits Long-Term Plan

The Michigan State Medical Society (MSMS) announced that it is endorsing the concept of Gov. Jennifer Granholm's *Michigan First Health Care Plan* to help provide health care for Michigan's 1.1 million uninsured.

"A long-term goal of the Michigan State Medical Society is universal health care coverage - in one form or another - for all Michigan residents," said MSMS President Paul Farr. "This program would be a move in the right direction toward ensuring access to care for everyone."

Since the state still needs to obtain a federal waiver to make *Michigan First Health Care Plan* viable, MSMS stressed that it was only endorsing the program in concept at this point. More federal tax dollars need to come back to Michigan to help pay for the program for it to happen.

The Michigan First Health Care Plan was first announced by Gov. Granholm in this year's State of the State Address, and according to its billing would eventually cover between 550,000 and 1 million people who currently have no health insurance.

BEWARE OF "PHARMING"

Internet Scams Rampant

Consumers who conduct on-line financial transactions should be aware of an Internet scam known as "pharming," an attempt to steal personal information by redirecting computer users from legitimate commercial Web sites to fake sites set up by the scammers. These bogus Web sites copy logos and trademarks, often appearing identical to a financial institution's legitimate site.

By doing so, they trick consumers to click on a phony link, directing you to the imposter site. They'll then ask users to enter their login name, password, or other sensitive personal information, capturing the data for their own use.

Pharming works several different ways. Sometimes the thief infects a computer with a virus. When the Internet user tries to access the Web site of his or her financial institution, the computer is instead directed to a fake site. Once in a while, crooks actually hack in to the Web server of a financial institution's Internet Service Provider and change the address of the company's Web site to the address of a fake site. In both instances, the bandit is able to capture personal information without the Internet user suspecting any wrongdoing. Some pharmers also send out random e-mails made to appear like they come from your bank or Paypal, asking you to click on a link to your account in order to remedy a misunderstanding.

In order to avoid becoming a victim on pharming, the Attorney General recommends the following:

- Remember that when you are visiting a supposedly secure area of a Web site, the Web address in your browser will begin with HTTPS, which indicates a secure Web site, not just HTTP, which is indicative that a site is not fully encrypted.

- Double click on the padlock icon in your Web browser to see who owns the security certificate for a Web site. An illegitimate site either will not have a certificate, or the certificate will be owned by an entity that appears to be unrelated to the legitimate entity.

- If while visiting a Web site with an HTTPS address, you receive a message from your browser indicating that the Web site's certificate does not match the address being visited, never click "Yes" in response to the security alert question, "Do you want to proceed?" Instead, always click "No" in such instances.

- Install and update personal firewall programs on your computer. This will protect against the more common virus-infection type of pharming attacks.

- Regularly run anti-virus and anti-spyware programs.

- Check for available software security updates to your operating system and for commercial software programs.

A copy of the Consumer Alert and additional information on Identity Theft are both available from the Consumer Protection Division by calling 1-877-SOLVE-88 (1-877-765-8388) or by accessing the Attorney General's Web site http://www.michigan.gov/ag.

WIT, WISDOM, ETC . . .

Quotables

"Nobody on his deathbed ever said, "I wish I had spent more time at the office. . ."

-Paul Tsongas

"The government is becoming the family of last resort."

-Jerry Brown

Quote of the Week: Stephen Colbert

"Facts are like Sansabelt slacks, adjustable to fit your needs."

All Michigan legislation can be tracked at http://www.legislature.michigan.gov/ .

If you'd like to be removed from this distribution list, simply reply to this e-mail with "remove" in the subject header.

State Senator Gilda Jacobs represents the 14th Senate District, which includes Beverly Hills, Bingham Farms, Farmington, Farmington Hills, Ferndale, Franklin, Hazel Park, Huntington Woods, Lathrup Village, Oak Park, Pleasant Ridge, Royal Oak Township, Southfield, and Southfield Township. She is the Minority Vice Chair of the Families & Human Services Committee and the Economic Development, Small Business & Regulatory Reform Committee. She also serves on the Government Operations and Health Policy Committees.

Constituents of the 14th District may contact Senator Jacobs at sengjacobs@senate.michigan.gov or toll-free at 1-888-937-4453.

This newsletter is produced in single-space form in order to save paper and transmission costs.

####

Matthew J. Levin
Legislative Director
Senator Gilda Z. Jacobs
P.O. Box 30036
Lansing, MI 48909-7536
(517) 373-7888
mlevin@senate.michigan.gov